ELSEVIER

Computer Communications 22 (1999) 1351–1363

computer communications

Towards electronic commerce via science park multi-Extranets

A. Pakstas

University of Sunderland, School of Computing, Engineering and Technology, Sunderland SR1 3SD, UK

Abstract

This paper is devoted to examining of the new emerging area of the Internet use, namely, 'Extranets'. This is often referred as a 'third wave' of the universal Internet. Definitions and examples of Extranet are given. Extranets are compared with better known intergroupware and the concepts of *Communications*, *Collaboration*, and *Co-ordination* are illustrated. The notion of a multi-Extranet is introduced as a special case typically found in the Science Park (SP) environments. Three types of organizations using the facilities of the SP and having different relationships with its multi-Extranet are distinguished as follows: (a) 'normal' firms which will have their own Intranets and access to the Internet either on their own or via SP facilities; (b) 'small' firms, which will obtain access to the Internet via SP facilities and with the only Intranet, which will be actually Extranet; (c) 'large' firms which, perhaps, will not bother to connect to the SP facilities at all. Open application standards are discussed and a suite of standards supported by the consortium established by Netscape Communications is briefly presented. The roles of network management and associated security issues are outlined as crucial for the success of electronic commerce. The existing experience of running Intranets is discussed and accepted as applicable for Extranets and criteria are identified for choosing a planning strategy for the building of Extranets. Based on the existing experience, the 'top 5" problems have been identified such as *Internal Information Exchange*, *Discussions*, *Line-of-Business Applications*, *Collaborations* and *Link to Partners*. Typical cost items are identified and cost models are discussed for the cases such as cost of running Web-sites of various complexity, access expenses for mobile users/workers (via mobile telephones and ISDN connections) as well as losses caused by the downtime. Two typical phases for the building of an Extranet are suggested: (1) is focusing on the applications and standards which will help to solve the above mentioned 'top 5' problems, and (2) is devoted to future development of the Extranet and 'flourishing' of the links with the customers as well as electronic commerce facilities.

Keywords: Enterprise networks; Extranets; Open standards; Network management and security; Cost models

1. Introduction

The Internet is flourishing and the World Wide Web is growing at an exponential rate. The possibility of the 'address crisis' was removed for the foreseeable future by the development of version 6 of the Internet Protocol (IPv6) to replace version 4. A fundamental concept of *Intranet*, the so-called *second wave*, was introduced only a few years ago. During 1996, Intranets have been embraced by corporate users of information services and made substantial inroads in strategic vision documents and procurement practices.

The new era of the *Extranet* or the *third wave* of the universal Internet concept has just begun. As a powerful enabler of worldwide electronic commerce, the Extranet is poised to trigger a revolution in the structure and operation of commercial enterprises and government organizations. Is it really a new idea with all of a set of totally new problems related to it? Or it is only a new word for something that we have already had for years? Some authors say that Extranets have been around since the first rudimentary LAN-to-LAN networks began connecting two different business entities together to form WANs and that in its basic form, an Extranet is the interconnection of two previously separate LANs or WANs with origins from different business entities [1]. But whatever are the views, it is becoming more and more popular—it was predicted that by 1998 the annual expenditures on Internet, Intranet and Extranet technologies will exceed US$8 billion [2]. Additionally, a recent Computer Economics survey on information systems spending found that 88% of organizations expect to make investments to expand networking capability over the next 12 months [3].

It is normally said that an Extranet, or extended Internet, is a private business network of several co-operating organizations located outside the corporate firewall. An Extranet service relies on the existing Internet interactive infrastructure, namely servers, E-mail clients and Web browsers. In comparison with the creation and maintenance of a proprietary network this feature makes Extranet very economical. Business partners, suppliers and customers who share common interests may form a tight business relationship and a strong communication bond. Web-systems have developed their content and marketing potential and

E-mail address: a.pakstas@ieee.org (A. Pakstas)

0140-3664/99/$ - see front matter
PII: S0140-3664(99)00132-2

Table 1
Summary of the Internet, Intranet and Extranet features

	Internet	Intranet	Extranet
Users	Everyone	Members of the specific firm	Group of closely related firms
Information	Fragmented	Proprietary	Shared in closely trusted held circles
Access	Public	Private	Semi-private
Security mechanism	None	Firewall, encryption	Intelligent firewall, encryption, various document security standards

in this sense the term 'third wave' also refers to the maturity process in the development of Web technology.

This article presents some results of the studies on the development of the Extranet for the high-technology science park. *Sørlandets Teknologisenter (STS)* in Grimstad, Norway is used as an example. The rest of the article is organized as follows. Definitions of terms are presented in Section 2. Applicable standards are discussed in Section 3. A role of Network Management is outlined in Section 4. Section 5 is devoted to security issues. Section 6 discusses experience and recommendations for the running of Intranets. Cost-relevant issues are presented in Section 7 and conclusions in Section 8.

2. Extranets: definitions and examples

We would like to start the definitions with the following sentence: unlike the Internet, an Extranet is not wide open. Unlike an Intranet, it is not restricted to internal use. An Extranet is a state of mind, not a technology [4]. There is a common understanding that an Extranet is a collaborative network that uses Internet technology to link businesses with their suppliers, customers, or other businesses that share common goals e.g. to allow customers and/or mobile workers access to the company's data. Thus, an Extranet, or software that facilitates intercompany relationships, can be viewed as a part of a company's Intranet that is made accessible to other companies or that is a collaboration with other companies. The shared information might be accessible only to the collaborating parties or, in some cases, may be made public.

2.1. Examples of Extranet applications

The most obvious examples of Extranet applications are the following:

- Shared product catalogues accessible only to wholesalers or those 'in the trade'.
- Private *newsgroups* that co-operating companies use to share valuable experiences and ideas.
- Groupware in which several companies collaborate in developing a new application program they can all use.
- Project management and control for companies that are part of a common work project.
- Training programs or other educational material that companies could develop and share.

Thus, a term 'Extranet' refers to an Intranet that is partially accessible to authorized outsiders. Whereas an Intranet resides behind a *firewall* and is accessible only to people who are members of the same company or organization, an Extranet provides *various levels of accessibility to outsiders*. An individual can access an Extranet only if:

- He/she has a valid *username* and *password*, and
- The user's identity determines which parts of the Extranet can be viewed/accessed.

Finally, Table 1 summarizes the discussed features of Internet, Intranet and Extranet.

Thus, we conclude that Intranets and Extranets are rather *classes of applications* than *categories of networks*. Applications in the public Internet, Intranet, and Extranet will all run on the same type of network infrastructure, but their software and data content resources will be *administered* for different levels of accessibility and security.

2.2. New term for intergroupware?

Workgroups may often need special tools for *Communications*, *Collaboration*, and *Coordination*, *which* are referred as *groupware* [5]. Emphasis is on computer-aided help to implement message-based human communications and information sharing as well as to support typical workgroup tasks such as scheduling and routing of the workflow tasks.

In a typical enterprise communications the inter- and intra- organizational media-based communications activities are forming two separate parallel *planes* [5]. The dimensions of each plane are the degree of *structure* and the degree of *mutuality* in the communications activities. *Structure* lies between informal (ad-hoc) and formally structured, defined, and managed or edited processes. *Mutuality* ranges from unidirectional or sequential back-and-forth message passing, to true joint work or *collaborative transactions* in a shared space of information.

The resulting *four regions* characterize *four different kinds of interaction*, which place distinct demands on their media vehicles or tools. Separate tools have been developed in each region usually as isolated solutions, but the need to

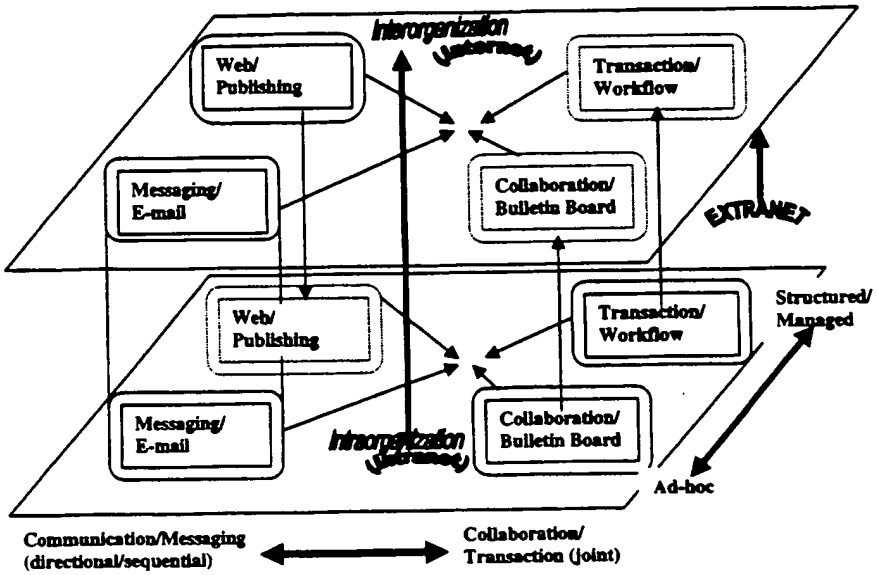

Fig. 1. Relations between Extranets and intergroupware.

apply them to the wide spectrum of electronic documents and in co-ordinated form is causing them to converge. Thus, we can describe groupware in terms of the following categories representing three of four identified regions. These are [5]:

- Communications or messaging (notably E-mail).
- *Collaboration or conferencing* (notably forums or 'bulletin board' systems which organize messages into topical 'threads' of group discussion, maintained in a shared database), and
- *Co-ordination or workflow and transactions* (applying pre-defined rules to automatically process and route messages).

Fig. 1 shows the distinct forms of electronic media

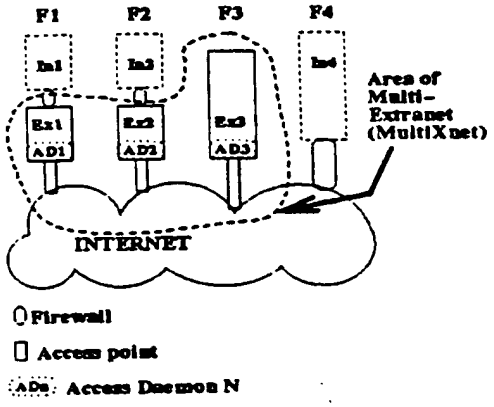

Fig. 2. Architecture of MultiXnet. Here: F1...F4—firms; In1, In2, In4—Intranets; Ex1, Ex2 and Ex3—Extranets.

supported by the groupware, the kinds of interactions they support, and how they are converging [5]. *Intergroupware* is just groupware applied with the flexibility to support multiple interacting groups, which may be open or closed, and which may share communications selectively, as appropriate (as in an Extranet). It should be noticed that Lotus Notes is one of the approaches to implement intergroupware and its success is based on the recognition of the fact that while these mentioned categories have distinct characteristics, they can only be served effectively by a unified platform that allows them to interact seamlessly.

2.3. Multi-Extranet as a new artifact

In many Science Parks (such as STS) there is often a mixture of the following three types of organizations which will use its facilities:

- 'Normal' firms which will have their own Intranets and access to the Internet either on their own or via STS facilities.
- 'Small' firms, which will obtain access to the Internet via STS facilities and with the only Intranet, which will be actually an Extranet.
- 'Large' firms such as Ericsson, Telenor, etc. perhaps, will not bother to connect to the STS facilities at all.

This situation is depicted in Fig. 2. Here F1 and F2 are examples of 'normal' firms, F3 is example of small firm and, finally, F4 is an example of a large firm.

Firewalls between Intranets In1, In2 and In4, and the Internet are in this case the property and responsibility of their owners. Extranets Ex1, Ex2 and Ex3, in contrast, are the responsibility of STS. In order to regulate the rights of

access to these Extranets for different categories of users it is presumed that *Access Daemon* should be provided for each Extranet. It is unclear on the current stage of study if some *Common Access Daemon* is feasible (i.e. such daemon which will function as a 'Yellow Page' service or common access interface for all the firms covered by STS services).

We suggest a new term such as *Multi-Extranet* (or *Multi-Xnet*) for this class of system. We expect that such studies will arise in similar environments of Hi-Tech Science Parks, Technological Incubators, etc. i.e. where many (often start-up) firms will share common infrastructures and at the same time will be interested in developing a common profile. In this case we can define STS's MultiXnet STSmXn as the superposition of the involved Extranets, i.e. STSmXn = Ex1 + Ex2 + Ex3 or in the general case for the Organisation O : 0mXn = SUM(Xi).

3. Open application standards

3.1. Standards and approaches

Broad use of the Internet technology in general and development of Extranets in particular is now supported by the existence of *the open application standards* that offer a range of features and functionality across all client and server platforms. Amongst those we would like to mention the following groups of standards:

- Platform-independent content creation, publishing and sharing of the information: HTML and HTTP.
- Platform-independent software development as well as the creation and deployment of distributed objects: Java, JavaScript, Common Object Request Broker Architecture (CORBA).
- Platform-independent messaging and collaboration (E-mail, discussion, and conferencing capabilities): Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Multipurpose Internet Mail Extensions (MIME), Secure MIME (S/MIME), Network News Transport Protocol (NNTP), Real Time Protocol (RTP).
- Directory and security services, network management capabilities: Lightweight Directory Access Protocol (LDAP), X.509, Simple Network Management Protocol (SNMP).

Obviously, there can be different approaches to the implementation of Extranets and first of all we would like to mention the initiative of *Netscape Communications* which offers a suite of applications (called 'AppFoundry') that it says are designed for possible Extranet use. Since here the term 'Extranet' puts a name on a phenomenon that already existed informally in various inter-company groupware it is pretty obvious that *Lotus Notes* is another candidate that would seem to support Extranets. EWOS is an open European organization working to provide high quality contributions to the worldwide efforts to build an effective Global Information Infrastructure, whilst ensuring proactive support of solutions meeting specific European needs, in areas such as Electronic Commerce should also be mentioned. In this article we will focus only on Netscape's approach.

3.2. Netscape's choice

Netscape's partners have agreed on a collection of standards and 'best practices' for use in Extranet deployment and creation of *Crossware*. For enterprises, this offers two significant benefits:

- An assurance of interoperability among products from multiple vendors.
- A virtual roadmap for efficient implementation of an Extranet.

Netscape's partners are committed to support the following Internet standards: LDAP, X.509 v3, S/MIME, vCards, JavaSoft, EDI INT (see Appendix A). Together, these standards create a comprehensive infrastructure that enables Crossware applications to interoperate across the Internet and the Intranets of business partners, suppliers, and customers.

They also serve to provide a secure environment that supports much more than simple exchange of HTML pages between enterprises. In fact, the standards agreed upon by Netscape's partners represent by far the most secure, as well as the best supported, open standards technology.

To summarize:

- Open standards provide the most flexible, efficient, and effective foundation for enterprise networking.
- Enterprise Intranets have exhibited clear benefits and are becoming ubiquitous.
- Netscape believes that Extranet technology represents the optimal future for enterprise networking.
- The claimed goal of Netscape and its partners is 'to assist enterprises in the deployment of secure, effective Extranets'.

4. Role of network management

As was mentioned in Section 1, enterprise applications in the Extranet (software and data content resources) must be *administered* for different levels of accessibility and security. *Network Management* refers to the broad subject of managing computer networks. Network management systems have been in operation for many years especially in their own *proprietary* worlds such as Netview, AT&T Accumaster and Digital Equipment Corporation's DMA. With the implementation of SNMP, local area and wide area network components could be monitored and 'managed'. Some systems are considered non-manageable

because they are only accessible by an RS-232 port and not by Netview or SNMP. Network Management for many means nothing but the monitoring and management of network *architectural hardware* such as routers, bridges and concentrators i.e. nothing above the network layer of the OSI model is considered manageable.

There is, however, a worrying situation that with the vast amount of raw data available, most of the IT Managers have no idea what they really want because, in part, they don't know what's available. An additional concern is about a suitable format for the data that is meaningful.

Another alarming trend to be mentioned here is that most of the Senior Network Engineers tend to spend funds on hardware and software *before* the real requirements are gathered and defined. Consequently, IT departments either spend very little on network management or they 'go for broke' with the huge hardware platforms and expensive artificial intelligence engines driving network management for the company.

4.1. Network management technologies

Network management covers a wide area, including:

- Security: ensuring that the network is protected from unauthorized users.
- Performance: eliminating bottlenecks in the network.
- Reliability: making sure the network is available to users and responding to hardware and software malfunctions.

The task of a management technology is to support the management of resources in a distributed environment—to enable a *manager system* to gather the information about the *resources* that are *managed* and to exercise *control* over *them*. These resources are typically in or under the direct control of some other computer system or system component, termed the *managed system* or *agent*, with which the manager system communicates. For example, in a CORBA environment, these system elements are *objects*.

Specifications of management technologies typically cover the *communications protocols* between manager and managed systems, and the *management information* that defines requests for management operations, the results of the operations and unsolicited reports such as alarms.

Existing Network and System Management solutions are based on different management technologies. The most common technologies are:

- OSI Management
- Internet Management
- CORBA/OMG.

In large enterprises (e.g. Telecommunication Service Providers), system and network managers have to deal with heterogeneous communication and information processing environments where more than one management technology is in use. Hence there is an urgent need for strategies for *coexistence* and *convergence* between the technologies.

4.2. Management in OSI

The OSI Management technology enables manager systems to monitor and control resources by sending operation requests to managed systems, and it enables managed systems to send event reports when important things happen to the resources. It uses the OSI CMIP protocol to carry the management information over a data communication network. CMIP may be supported by a full 7-layer OSI stack or by other means.

The OSI management information model uses an object-oriented approach to represent how real-world systems and resources can be managed, in the form of *managed objects*, which are defined using the ISO/IEC & ITUT Guidelines for the Definition of Managed Objects (GDMO), together with Abstract Syntax Notation One (ASN.1). It has mechanisms for increased efficiency that make it possible to send a number of operation requests in a single communication, to filter out less significant event reports under management control, to log events locally, and to summarize information.

OSI management also includes a number of specifications aimed at increasing consistency in the way different resources are managed, such as a common format for alarms and a common state model. These are called *systems management functions*.

4.3. Management in IP-network

There are few recommendations (RFCs) specified by the IETF that define how network management is to work in the TCP/IP environment. Its basic protocol is SNMP (Simple Network Management Protocol), with a third version, SNMPv3, now under development [6].

The Internet Management model adopts a manager/agent approach where the agents maintain information about resources and managers request information from the agents. The Internet Structure of Management Information (SMI) standard specifies a methodology for defining the management information contained in the Management Information Base (MIB). SMI uses a subset of ASN.1 data types. The MIB defines the elements of management information as variables and tables of variables.

Adding new features to SNMP, as it is defined in the versions SNMPv2 and SNMPv3, brings it closer to the OSI management philosophy and it seems that 'Simple' in the title of the protocol is going to be changed to 'Sophisticated'.

4.4. Management in CORBA/OMG

An object-based environment for the development of distributed systems, which includes CORBA (the Common Object Request Broker) and IDL (an Interface Definition Language) for specifying the interface to objects has been

developed by the Object Management Group (OMG). The initial release of CORBA does not specify as such any particular *protocol* for communication between *objects* that are in different *systems* but assumes use of a standardized protocol (although later versions of CORBA will specify particular protocols).

There is, however, an opportunity to use CORBA IDL to specify objects related to management. Some of the CORBA services such as Naming and Event can also be directly used for building the management functions.

4.5. Convergence of the network management technologies?

Various approaches are under way to show how the diverse technologies that have been developed can coexist, and perhaps converge to provide a single management environment.

One important activity is directed to the building of gateways between networks using OSI and Internet Management technologies. For example, the *specification* (developed by the NMF) of a simple *mapping* between managed objects defined using GDMO and those defined using Internet SMI has been developed.

The Joint Inter-Domain Management (JIDM) task force with membership from the NMF and X/Open is another body working towards harmonization of the network management issues. Their document *Inter-Domain Management Specifications, Specification Translation*, which is currently an X/Open preliminary specification, specifies translation algorithms for converting between the CORBA IDL objects and OSI GDMO managed objects (in both directions), and between SNMP MIBs and CORBA IDL (only in one direction). Future work will specify the dynamic conversion requirements e.g. how to convert CMIP PDUs for operation with CORBA objects.

5. Network security issues

Most often regardless of the business type, sufficient number of users on many of the private networks are demanding access to the Internet services such as the World Wide Web (WWW), Internet mail, Telnet, and File Transfer Protocol (FTP). Additionally, some corporations want to offer WWW home pages and FTP servers for free public access on the Internet. Thus, exposing of the organization's private data and networking infrastructure to the Internet crackers definitely increases concerns of the Network Administrators about security of their networks [7]. It has been very well expressed that *'security should not be a reason for avoiding cyberspace, but any corporation that remains amateurish about security is asking for trouble'* [8].

A rise in external access is coming from telecommuters, business associates, customers, or potential customers, each with a unique set of computing and data requirements. The solution will not and should not be the same for all [9]. Choosing the best Extranet solution for a company's needs is important. To choose the correct solution, it is important to understand clearly the available alternatives. There can be identified six basic Extranet components as well as some specialized and hybrid solutions [9]: (1) access to the external resources; (2) Internet protocol (IP) address filtering; (3) authentication servers; (4) application layer management; (5) proxy servers; and (6) encryption services. Each is sufficient to initiate business communications, but each carries different performance, cost, and security. Namely security (as recent statistics shows [10]), is the main issue preventing organizations from establishing Extranets.

The term *security* in general refers to techniques for ensuring that data stored in a computer cannot be read or compromised. Obvious security measures involve *data encryption* and *passwords*. Data encryption by definition is the translation of data into a form that is unintelligible without a deciphering mechanism. A password, obviously, is a secret word or phrase that gives a user access to a particular program or system. Thus, in the rest of this section we will focus on the following issues: risk assessment, development of the security policy, and establishment of the authentication, authorization and encryption.

5.1. Risk assessment

Risk assessment procedures should answer the following typical questions:

- What are the organization's most valuable intellectual and network assets?
- Where do these assets reside?
- What is the risk if they are subjected to unauthorized access?
- How much damage could be done—can it be estimated in terms of money?
- Which protocols are involved?

5.2. Security policy

To provide the required level of protection, an organization needs a security policy to prevent unauthorized users from accessing resources on the private network and to protect against the unauthorized export of private information. Even if an organization is not connected to the Internet, it may still want to establish an internal security policy to manage user access to portions of the network and protect sensitive or secret information. According to the FBI, 80% of all break-ins are internal.

Policy is the allocation, revocation, and management of permission as a network resource to define who gets access to what [11]. Rules and policy should be set by business managers, the Chief Information Officer and a security specialist—someone who understands policy writing and

the impact of security decisions. Network managers can define policy for a given resource by creating an entry in access control lists which are two-dimensional tables that map users to resources.

A firewall is an implementation of *access rules*, which are an articulation of the company's security policy. It is important to make sure that some particular firewall supports all the necessary protocols. If LANs are segmented along departmental lines, firewalls can be set up at the departmental level. However, multiple departments can often share a LAN. In this case, the creation of a *virtual private network (VPN)* for *each* person is highly advisable.

The following are recognized as the basic steps for developing a security policy:

1. Assessment of the types of risks to the data will help to identify weak spots. After correction, the regular assessments will help to determine the ongoing security of the environment.
2. Identification of the vulnerabilities in the system and possible responses, including operating system vulnerabilities, vulnerabilities via clients and modems, internal vulnerabilities, packet sniffing vulnerabilities and means to test these vulnerabilities. Possible responses include encrypting data and authenticating users via passwords and biometrically.
3. Analysis of the needs of user communities:
   - Grouping data in categories and determining access needs. Access rights make the most sense on a project basis.
   - Determining the time of day, day of week and duration of access per individual are the most typical procedures.
   - Determination and assignment of the security levels can include the following, five levels:
     - *level one* for top-secret data such as pre-released quarterly financials or a pharmaceutical firm's product formula database;
     - *level two* for highly sensitive data such as the inventory positions at a retailer;
     - *level three* for data covered by non-disclosure agreements such as six month product plans;
     - *level four* for key internal documents such as a letter from the CEO to the staff;
     - *level five* for public domain informationIn order to implement this security hierarchy it is recommended that firewalls are put at the personal desktop, workgroup, team, project, application, division, and enterprise levels.
4. Writing the policy.
5. Development of a procedure for revisiting the policy as changes are made.
6. Writing an implementation plan.
7. Implementation of the policy.

5.3. Authentication, authorization, encryption

When it comes to the security aspects of teleworking and remote access, in all aspects of information technology security, there is a tension between the goals of the participants. Users want access to information as quickly and as easily as possible. Whereas information owners want to make sure that users can only access the information they are allowed to. Security professionals often find it difficult to reduce this tension because of the demands of users in a rapidly changing business world. Smartcards may provide the solution for this problem [12].

Involving encryption requires introduction of the key *management/updating procedure*. Encryption can be implemented:

- *At the application*: Examples of this are Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME), which provide encryption for E-mail.
- *At the client or host network layer*: The advantage of this approach is that it will provide extra protection for the hosts that will be in place even if there is no firewall or if it is compromised. The other advantage is that it allows distribution of the burden of processing the encryption among the individual hosts involved.
  This can be done on the client with products such as Netlock (see Ref. [13]), which provides encryption on multiple operating system platforms at the IP level. A system can be set up so that it will only accept encrypted communications with certain hosts. There are similar approaches from Netmanage, and FTP Software.
- *At the firewall network layer*: The advantage to this approach is that there is centralized control of encryption which can be set up based on an IP address or port filter. It can cause a processing burden on the firewall, especially if a lot of streams have to be encrypted or decrypted. Many firewalls come with a feature of *virtual private network (VPN)*. VPNs allows encryption to take place as data leaves the firewall. It has to be decrypted at a firewall on the other end before it is sent to the receiving host.
- *At the link level*: The hardware in this case is solely dedicated to the encryption process, thus off-loading the burden from a firewall or router. The other advantage of this method is that the whole stream is encrypted, without even a clue as to the IP addresses of the devices communicating. This can only be used on a *point to point link*, as the IP header would not be intact which would be necessary for routing.

Products like those manufactured by Cylink (see Ref. [14]) can encrypt data after it leaves the firewall or router connected to a WAN link.

Extranet routers combine the functions of a virtual private network (VPN) server, an encryption device and a row address strobe [15]. The benefits of using the Extranet

Table 2
Weak points and security hazards

Weak point/hazard	Technical solution
Operating system/ applications on servers	Research vulnerabilities; monitor CERT advisories; work with vendors; apply appropriate patches or remove services/ applications; limit access to services on host and firewall; limit complexity
Viruses	Include rules for importing files on disks and from the Internet in security policy; use virus scanning on client, servers and at Internet firewall
Modems	Restrict use; provide secured alternatives when possible (such as a dial-out only modem pool)
Clients	Unix: Same as server issues above; Windows for workgroups, Win95, NT: Filter TCP/UDP ports 137, 138, 139 at firewall; be careful with shared services, use Microsoft's service pack for Win95 to fix bugs
Network snooping	Use encryption, isolate networks with switch or router
Network attacks	Internet firewall; Internal firewall or router; simple router filters that do not have an impact on performance
Network spoofing	Filter out at router or firewall

routers includes the network's ability to build secure VPNs and tunnel corporate Internet protocol traffic across public networks like the Internet. Management is a lot easier than it is in a multivendor, multidevice setup. Expenses are a whole lot lower, since there is no need for leased lines.

5.4. Summary of the weak points and security hazards

Finally, Table 2 provides a summary of the weak points in the system security, identifies and shows how these problems can be addressed and suggests technical solutions for them. Additional information for various platforms can be obtained in Refs. [16–20].

6. Experience and recommendations for running of Intranets

6.1. Intranet applications and their obstacles

Delphi Consulting Group, which is a company advising large and small corporations on the directions of their document management strategies, has reported results of their survey on installed Intranet applications. In Delphi's recent survey [21] of over 600 users/evaluators of electronic document management systems, 65% had Intranets in place and only a mere 6% had no plans to install an Intranet over the next two years. Currently, less than half of all organizations surveyed had more than 50% of their desktops connected to an Intranet. But, these organizations projected that by the year 2000 (three years away), over 82% of all organizations will have 75% or more of their users connected to an Intranet.

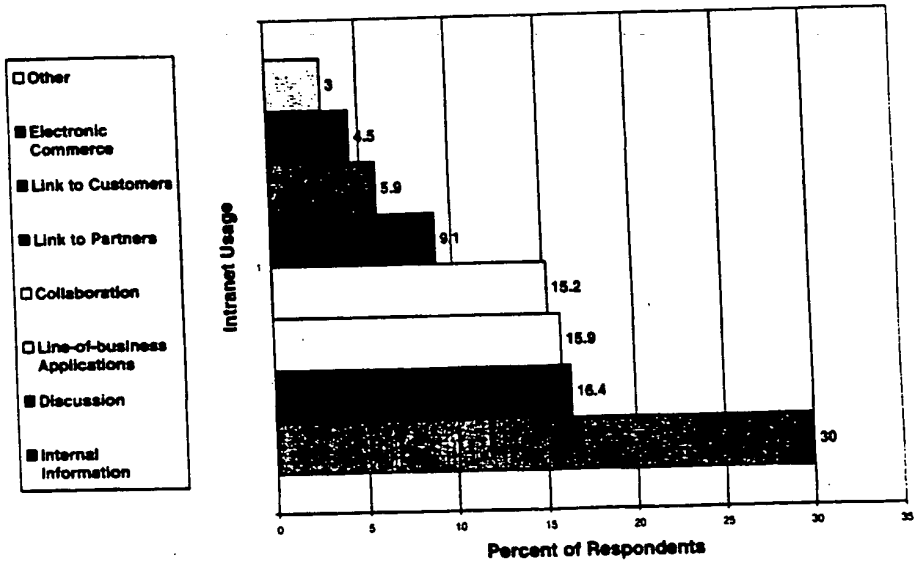

Fig. 3. Installed Intranet applications.

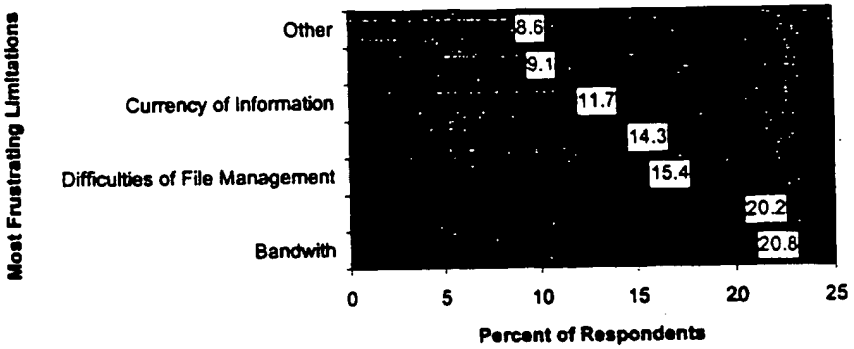

Fig. 4. Current obstacles to Intranet applications.

The most common usage of the Intranet among those organizations surveyed by Delphi was as a means to share internal information (see Fig. 3). However, amongst all of the widespread acceptance and positive outlooks expressed by the survey respondents, caution regarding frustrations and hurdles to Intranet acceptance were also expressed (see Fig. 4).

As might be expected, the eternal problem of bandwidth capacity topped the user's list of frustrations. But this problem can be easily dealt with, and will surely be met by various 'solutions' from hardware and telecommunications vendors in a relatively short time frame. A more significant set of problems dealing with the practical aspects of developing meaningful mission critical applications over the Intranet fall just beneath the bandwidth dilemma. These range from the inability to integrate Web-based applications and legacy systems, to the vulnerability of Intranet information (e.g. security and currency).

6.2. Criteria for choosing a planning strategy

Delphi's survey presented above covers a much wider group of companies than we ever can expect at the STS-600 surveyed by Delphi vs. ca. 100 expected in STS in the coming two years. Thus, we can accept practice observed by the survey as a representative set for future considerations.

Furthermore, based on Delphi's survey we suggest that it might be reasonable to focus on the *'top 5'* approach, i.e. select 5 upper parameters shown in the diagrams as guidelines for our choices. In this case a diagram 'Installed Intranet Applications' helps us to identify the most important usage of Intranets/Extranet: *Internal Information Exchange, Discussions, Line-of-business Applications, Collaborations* and *Link to Partners*.

Surprising enough is the fact that other two, such as *Link to Customers* and *Electronic Commerce* (which according to common definition sounds vital for any Extranet) does not fall into the category of most important Intranet usage! Not yet...

Considering the observed limitations of Intranets we note that here the 'top 5' group identifies the following problems: *Bandwidth, Integration with Existing Systems, Difficulties of File Management, Security* and *Currency of Information*.

The *bandwidth* problem can be solved relatively easily. *Integration with Existing Systems, and Difficulties of File Management* are problems of the same nature caused by bringing 'un-networked' organization to the Intranet. It can be completely solved by choosing appropriate application standards and tools.

The *security* problem while will be essentially resolved by appropriate protocols and tools but will still require regular activity of network managers who are responsible for it. The last problem, *Currency of Information*, is rather organisational which, perhaps will stay unsolved forever if no appropriate information/document flow management policies and tools are applied by the organization.

7. Cost issues: facts and models

This section will examine cost-relevant issues important for the infrastructure and operation of Extranets and Multi-Xnets such as STS. First we look at the cost of running a Web-site and then at the access expenses for mobile users/workers. Finally, losses caused by the downtime are discussed.

7.1. Cost of running web site

The evolutionary scale of Web sites suggested by the Positive Support Review Inc. of Santa Monica, CA [22] includes the following:

1. *Promotional*: A site focused on a particular product, service or company. Cost: US$300 000 to US$400 000 per year (17–20% on hardware and software, 5–10% on marketing, and the balance on content and servicing).
2. *Knowledge-based*: A site that publishes information that is updated constantly. Cost: US$1 to US$1.5 million annually (20-22% on hardware and software, 20–25% on marketing, and 55–60% on content and servicing).

3. *Transaction-based*: A site that allows surfers to shop, to receive customer services or to process orders. Cost: US$3 million per year (20–24% on hardware and software, 30–35% on marketing, and 45–50% on content and servicing).

A similar classification by Zona Research Inc. of Redwood City, CA (cited in Ref. [23]) divides Web sites into:

1. *Static presence ('Screaming and Yelling ')*. According to Zona Research, page cost for such sites is less than US$5000. At present, the absolute majority of Web sites belong to this category.
2. *Interactive ('Business Processes and Data Support')*, with page costs ranging from US$5000 to US$30 000. Perhaps 15–20% of all current Web sites are in this category.
3. *Strategic ('Large Scale Commerce')*, with dynamic pages that cost more than US$30 000 each to produce and maintain. Currently less than 0.5% of all Web sites are in this category.

Thus, electronic commerce sites are not toys and before entering to these *WWWaters* an organization must develop clear ideas about current and strategic investments to this part of their business. Nevertheless, in its latest market research report (see Ref. [24]) Zona projects multibillion dollars Intranet/Extranet market expansions till the end of the century.

7.2. ISDN cost model

The mobile workers should look at ISDN as an important technology for building Extranet infrastructure because of its ability to support flexible access. The ISDN cost model should consider the following:

- Service fees from local telecoms company for each location (installation + monthly + per min)
- Long distance charges, if applicable
- Cost of equipment (NT1+TA, NT1+bridges, NT1+routers, etc.)
- Cost of Internet Service Provider (ISP) services, if applicable.

Thus, planning a budget for a month, for, example, will include US$25 a month + 2 cents per minute per channel. Therefore, it is US$2.40 per hour for two B connections. If a user needs to be connected three hours per day, 20 days per month, it will cost US$ 144 + 25 = 169 for a month of service, just for the local telecom portion of your ISDN connection. Long distance fees and ISP charges would naturally need to be factored into this as well.

7.3. Mobile connection cost model

Mobile workers can consider wireless communications as another option that can be highly cost effective, but its costs are generally *higher* than wireline communications. We would like to remind the reader, that with packet data the modem occupies the radio channel only for the time it takes to transmit that packet. In ordinary data networks users are usually billed for the amount of data they send. In contrast, for data communication over a wireless link there is a established *circuit connection* and *payment is based on the duration* of the call just as with an ordinary voice call. The per-minute charges are usually the same.

Wireless modems are complex electronic devices, containing interface logic and circuitry, sophisticated radios, considerable central processing power and digital signal processing. As such, they cost more than landline modems. Most wireless WAN modems cost US$500 or more.

7.4. Cost of downtime

Electronic commerce is difficult when the infrastructure is unreliable. In this section we will use an example from Ref. [25] to examine the cost of downtime for some consumer-oriented business, such as an airline or hotel reservation centre. If customers have a choice then they will call a competitor and place their order there.

We will use an example where the customer service centre has a staff of 500 people, each of which carries a burdened cost of US$25 an hour. They make an average of 60 transactions per hour and average of three high-priced sales per hour. Hours of operation are 24 hours a day, seven days a week, 365 days a year.

In actuality, the line managers of the site should calculate the costs of downtime, not the IT staff. However, this information is often not forthcoming. So, this example can be presented to give a general sense of the impact that downtime has on the bottom line. The goal is to open some eyes and generate some debate. We can use this example as a guideline for how to estimate the cost of outages in our environment.

As we can see (Tables 3–5), the cost of outages in the hypothetical network with an availability rate of 99.9% is about half a million dollars a year. If hardware and software necessary to do the job is already bought then *we can consider this estimate as a guideline for the additional budget to spend on providing redundancy*. This is separate and apart from the funds required to provide a base level of network functionality. Thus, it is really not worth rushing headlong into designing a fault-tolerant network unless all parties agree on all the implications that downtime has on the operation.

7.5. Economical effectiveness of Extranets

While there are already many publications about conceptual or technical aspects of Extranets it is difficult to identify those which look to the same problems from the more focused, economical point of view. We will discuss here some of the research which we found relevant.

BNSDOCID: <XP__4179336A__1_>

Table 3
Cost of outages

Downtime percentage	0.9990
Number of hours/year	8.76
Number of employees	500
Average burdened cost	825
Idle sale	US$109 500
Impact to production	US$131 400
Opportunity lost	US$262 500
Total downtime impact	US$503 700

The choice of criteria for building of Extranets could be influenced by the results obtained in the research focused on the competitive advantage achieved by using internet, Intranet and Extranet applications [2]. The competitive advantage achieved by using these technologies can be measured over the seven dimensions of the CAPITA (Competitive Advantage Provided by an Information Technology Application) measurement i.e. *primary activity efficiency*, *support activity efficiency*, *resource management functionality*, *resource acquisition functionality*, *threat*, *preemptiveness*, and *synergy*. Internet, Intranet, and Extranet applications could be measured for their contribution on each dimension of competitive advantage. This research is undergoing and no particular results are available as yet.

Research presented in Ref. [26] is intended to show through a case study how the Extranet has been used by one specific company to significantly reduce operating costs. The activities of the company are analyzed within the framework of the value chain concept developed by Porter. This, it is felt, will provide a greater insight into how the Extranet can be used to improve profit margins. Prior research in this area has either been of a conceptual nature (explaining theoretically how the Extranet should be employed) or of a survey nature (examining, by means of a survey instrument, the benefits accruing to companies that have adopted the Extranet). This study is different in that it examines in detail, by means of a case study, how the Extranet influences a retail company's chain of activities.

8. Conclusions

Currently the Extranet is conceptualized as the key technology, which can enable development of the third wave of electronic commerce sites. While technical and cost advantages are of very high importance, the real significance of the Extranet is that it is the first *non-proprietary* technical tool that can support rapid evolution of *electronic commerce*.

Table 4
Impact to production

Profit per transaction	0.5
Transactions per hour per employee	60
Missed transactions per hour	30 000
Total missed transactions	262 800
Impact of missed transactions	US$131 400

It is already clear that the Internet has impacted on retail sales through the use of credit cards and various digital cash and payment settlement schemes. However, the experts predict that the real revolution over the next three to five years will be in systems for global procurement of goods and services at the wholesale level and that the role of Extranets is crucial to this. It is also expected that on a more fundamental level the Extranets will stimulate the business evolution of conventional corporations into *knowledge factories*.

Before planning MultiXnet development phases for the STS we should admit that STS is already behind most of the most active participants of the Intranet/Extranet implementation process. However, the rate of deployment of Extranets is currently minimal and this fact gives a chance to liquidate the gap reasonably quickly. Given the relative immaturity of the Intranet itself, it is reasonable to predict that great strides will be made in this area within the next two years.

Thus, it seems natural that we allocate 12 months for the implementation of **Phase I** and another 12 months for **Phase II**. It is reasonable for **Phase I** to focus on the applications and standards which will help to solve the identified 'top 5' problems. Most important for the STS is the development of the IT infrastructure, access to the system for the mobile workers and partners inside the park, a common Web-server, the normally working Intranets in the all partner companies and a common E-mail server.

Phase II is devoted to future development of the Extranet. Development of links with the customers as well as electronic commerce facilities should not be forgotten but its 'flourishing' can be planned for the second Phase. After the first two years of such a plan, STS will hopefully liquidate a gap and will find itself at the same stage of development as other *Intranet-active* communities and countries.

Acknowledgements

This project was partially funded by Agder College, Grimstad, Norway.

Appendix A. Internet standards supported by Netscape's partners

A.1. LDAP

LDAP: intelligent directory services store and deliver contact information, registration data, certificates, configuration data, and server state information. These services provide support for single-user logon applications and strong authentication capabilities throughout the Extranet.

Table 5
Opportunity lost

Profit per sale	20
Sales per hour per employee	3
Missed sales per hour	1500
Total missed sales	13 140
Impact of missed sales	US$262 600

Key benefits:

- Users can search for contact information across enterprises, partners, and customers using the same interface and protocols as internal corporate directories.
- A standard format for storage and exchange of X.509 digital certificates allows single-user logon applications and secure exchange of documents and information via S/MIME.
- Replication over open LDAP protocol allows secure distribution of directory data between enterprises.
- Enables Extranet applications that rely on fast and flexible queries of structure information.

A.2. X.509 v3

X.509 v3 digital certificates provide a secure container of validated and digitally signed information. They offer strong authentication between parties, content, or devices on a network including secure servers, firewalls, E-mail, and payment systems. They are a foundation for the security in S/MIME, object signing, and Electronic Document Interchange over the Internet (EDI INT). Digital certificates can be limited to operate within an Intranet or they can operate between enterprises with public certificates co-issued by the company and a certification authority such as VeriSign. Certificates surpass passwords in providing strong security by: authenticating identity, verifying message and content integrity, ensuring privacy, authorizing access, authorizing transactions, and supporting non-repudiation. Key benefits:

- Digital certificates eliminate cumbersome login and password dialog boxes when connecting to secure resources.
- Each party can be confident of the other's identity.
- Digital certificates ensure that only the intended recipient can read messages sent.
- Sophisticated access privileges and permissions can be built in, creating, precise levels of authority for Internet transactions.

A.3. S/MIME

S/MIME message transmission uses certificate-based authentication and encryption to transmit messages between users and applications. S/MIME enables the exchange of confidential information without concerns about inappropriate access.

A.4. vCards

vCards provide a structured format for exchanging personal contact information with other users and applications, eliminating the need to retype personal information repeatedly.

A.5. JavaSoft

Signed objects allow trusted distribution and execution of software applications and applets as part of an Extranet. With signed objects, tasks can be automated and access to applications and services within the extended network granted based on capability. A digital certificate is used with a signed object to authenticate the identity of the publisher and grant appropriate access rights to the object.

A.6. EDI INT

This provides a set of recommendations and guidelines that combine existing EDI standards for transmission of transaction data with the Internet protocol suite. By using S/MIME and digital signatures, EDI transactions between enterprises can be exchanged in a secure and standard fashion.

References

[1] P.Q. Maier, Implementing and supporting extranets, Information-Systems-Security 7 (4) (1999) 52–59.
[2] M.G. Wells, Using Internet and Extranet applications for competitive advantage, Proceedings of the Annual Meeting of the Decision Sciences Institute, San Diego, CA, USA, Nov 22–25 1997. Decis. Sci. Inst., Atlanta, GA, USA 2 1997 628.
[3] Building a network for the future-implications of Internet applications on the enterprise networking infrastructure, Computer Economics: Networking Strategies, 6(12) (1998) 1–4.
[4] R.H. Baker, Extranets: The Complete Sourcebook, McGraw-Hill, New York, 1997.
[5] R.R. Reisman, Extranets and intergroupware: a convergence for the next generation in electronic media-based activity, Teleshuttle Corporation, http://www.teleshuttle.com/media/InterGW.htm, 1998.
[6] O. Cherkaoui, et al., An implantation of SNMPv3, in: ENCOM'98: Enterprise Networking and Computing Conference, June 7, 1998, Atlanta, GA, IEEE Comm. Soc., USA, 1998.
[7] R. Herold, S. Warigon, Extranet audit and security, Computer Security Journal 14 (1) (1998) 35–40.
[8] J. Martin, Cybercorp: the new business revolution, Amacom Book Division, 1996.
[9] S. Trolan, Extranet security: what's right for the business? Information-Systems-Security 7 (1) (1998) 47–56.
[10] T. Lister, Ten commandments for converting your intranet into a secure extranet, UNIX Reviews: Performance Computing 16 (8) (1998) 33–37.
[11] R. Thayer, Network security: Locking in to policy, Data Communications 27 (4) (1998) 77–80.
[12] D. Birch, Smart solutions for Net security, Telecommunications 32 (4) (1998) 53–54,56.
[13] Netlock Version 1.4.1, Interlink Computer Sciences, Inc., http://www.interlink.com/NetLOCK, 1998.
[14] Global Network Security Products, Cylink Corporation, http://www.cylink.com/products, 1998.

[15] E. Robers, Extranet routers: The security and savings are out there, Data Communications 27 (12) (1998) 9.
[16] S. Castano, et al., Database Security, Addison Wesley/ACM Press, Reading, MA/New York, 1995.
[17] R. Farrow, Unix Systems Security, Addision-Wesley, Reading, MA, 1991.
[18] NCSA's publication catalog, NCSA, http://www.ncsa.com/catalog/catgenerity.html, 1998.
[19] Netware security, ALC Press, http://alcpress.com/courses/nws.htm, 1997.
[20] S.A. Sutton, Windows NT security guide, Addision Wesley Developers Press, http://www.trustedsystems.com/NTBook.htm, 1996.
[21] C. Frappaolo, Intranets: they way to a wider tomorrow, The Delphi. Group, http://www.delphigroup.com/articles/1997/StateOfIntranets.html, 1997.
[22] V. Junalaitis, The true cost of the Web, PC Week Nov. 18 (1997) 85.
[23] E. Shein, Natural selection, PC Week Oct. 14 (1996) E2.
[24] Electronic Economy: Let's Get Ready to MMBL, Zona Research Inc., http://www.zonaresearch.com, 1997.
[25] Walsh, B., Fault-Tolerant networking, CMP Net, http://techweb.cmp.com/nc/netdesign/faultmgmt.html, 1996.
[26] M. Anandarajan, A. Anandarajan, H.J. Wen, Extranets: A tool for cost control in a value chain framework, Industrial Management and Data Systems 98 (3/4) (1998) 120–128.

Algirdas Pakstas received his MSc in radiophysics and electronics in 1980 from the Irkutsk State University, PhD in systems programming in 1987 from the Institute of Control Sciences and Professor title from the Agder College in 1997. Currently with the University of Sunderland where he is doing research in software engineering for distributed computer systems, communications engineering and real-time systems. He is active in the IEEE Communications Society Technical Committees on Communications Software, Enterprise Networking and Multimedia. Has published two research monographs and over 70 other publications. He is a senior member of IEEE and member of ACM and the New York Academy of Sciences.